PRAWA I OBOWIĄZKI PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE

1. Przypadki i zasady powierzania danych do przetwarzania

Podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu administratora danych. O celach i sposobach przetwarzania danych osobowych zawsze decyduje administrator tych danych. Podmiotem przetwarzającym będzie więc podmiot, który jest odrębnym od administratora bytem prawnym oraz wykonuje operacje przetwarzania danych w imieniu administratora danych. Prościej mówiąc, przetwarza dane na zlecenie administratora danych, w zakresie czynności, które teoretycznie administrator mógłby sam wykonywać, np. prowadzić księgowość, ale decyduje się na outsourcing takich usług.

Status podmiotu

Od powierzenia danych należy odróżnić pojęcie udostępnienia danych. W przypadku udostępnienia, dane osobowe przekazywane są innemu podmiotowi, który w stosunku do nich staje się odrębnym administratorem. W tym przypadku ten drugi, odrębny administrator nie działa na zlecenie i w zakresie określonym przez pierwotnego administratora, bowiem sam te cele wyznacza. W temacie rozróżniania podmiotów przetwarzających od odrębnych administratorów danych wypowiedział się Bawarski Urząd Krajowy ds. Nadzoru nad Ochroną Danych. Jest to jeden z niemieckich organów nadzorczych działających na poziomie krajów związkowych. Urząd ten podał przykłady sytuacji, w których dochodzi do powierzenia przetwarzania danych oraz takie, które za powierzenie nie mogą być uznane (patrz ramka). To przykładowe wyliczenie może być pomocne również dla polskich administratorów.

Obowiązek zawarcia umowy powierzenia

Ogólne rozporządzenie o ochronie danych osobowych (RODO) w motywie 81 oraz w art. 28 ust. 1 wymaga, aby administrator danych korzystał wyłącznie z usług takiego podmiotu przetwarzającego, który daje odpowiednie gwarancje spełnienia wymogów wynikających z unijnego rozporządzenia.

W literaturze przedmiotu przyjmuje się więc, iż wybór dokonywany przez administratora powinien być uważny, a współpraca z podmiotami niedającymi odpowiednich gwarancji wykluczona. Ciężar odpowiedzialności za dokonanie odpowiedniego wyboru spoczywa oczywiście na administratorze, a sama decyzja powinna być podejmowana z uwzględnieniem wiedzy fachowej, wiarygodności i zasobów, umożliwiających wdrożenie środków technicznych i organizacyjnych odpowiadających wymogom RODO, także w obszarze bezpieczeństwa. Przy czym powierzenie danych do przetwarzania może mieć charakter jednorazowy lub stały.

Powierzenie może odbywać się na podstawie umowy lub innego instrumentu prawnego, podlegających prawu Unii lub innego państwa członkowskiego. Stronami zawieranej umowy są administrator i podmiot przetwarzający. Zgodnie z art. 28 ust. 3 RODO umowa lub inny instrument prawny musi określać:

- przedmiot i czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora.

Podmiot przetwarzający musi również zagwarantować, że osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania tajemnicy, chyba że podlegają one takiemu obowiązkowi z mocy przepisów ustawowych. Ze względu na to, że za działanie tych osób odpowiada podmiot przetwarzający, uregulowanie sposobu zobowiązania do zachowania tajemnicy i zagwarantowanie jej respektowania obciąża właśnie ten podmiot.

RODO zobowiązuje podmioty przetwarzające do wdrożenia środków technicznych i organizacyjnych odpowiadających kontekstowi przetwarzania i zidentyfikowanemu ryzyku naruszenia praw lub wolności osób fizycznych. Ponadto podmiot przetwarzający zobowiązany jest wspierać administratora w realizacji praw przysługujących osobom, których dane są przetwarzane, czyli prawo: dostępu do danych, do przenoszenia danych, do żądania usunięcia lub ograniczenia przetwarzania. Musi także realizować obowiązki wynikające z art. 32–36 RODO, a odnoszące się do: bezpieczeństwa przetwarzania, zgłaszania naruszeń ochrony danych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków dla ochrony danych oraz uprzednich konsultacji. Temu też muszą służyć wdrażane przez podmiot przetwarzający odpowiednie środki techniczne i organizacyjne.

Umowa powinna regulować również kwestie postępowania z danymi osobowymi po zakończeniu jej trwania poprzez zobowiązanie podmiotu przetwarzającego do zwrotu wszelkich danych lub ich usunięcia. RODO dopuszcza wyjątek od tej zasady i pozwala na dalsze przetwarzanie danych przez podmiot przetwarzający niezależnie od zakończenia świadczenia usług w przypadku, gdy prawo UE lub prawo państwa członkowskiego nakazują dalsze ich przetwarzanie, a dokładniej przechowywanie danych osobowych, i wiążą one podmiot przetwarzający. Przepisy unijnego rozporządzenia umożliwiają administratorom danych przeprowadzenie kontroli wykonywania przez podmioty przetwarzające obowiązków wynikających z RODO, w zakresie przekazanych danych.

Administrator wraz z podmiotem przetwarzającym mogą również, w ramach zawieranej umowy powierzenia, dokonać innych ustaleń. Przykładowo unormować kwestie związane z ewentualnym odszkodowaniem przy naruszeniu przez podmiot przetwarzający przepisów w zakresie ochrony danych osobowych. Mogą zastrzec kary umowne w przypadku naruszenia przez podmiot przetwarzający postanowień umowy oraz wprowadzić szczegółowe zasady prowadzenia audytów lub inspekcji przez administratora. Możliwe jest też uregulowanie zasad współpracy z inspektorem ochrony danych podmiotu przetwarzającego. Strony mogą również podjąć decyzję o stosowanych środkach technicznych i organizacyjnych, których zastosowania żąda administrator, a także o możliwych sposobach zakończenia współpracy.

Odpowiedzialność podmiotów

Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia zasad opisanych w RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Administrator lub podmiot przetwarzający mogą się zwolnić z takiej odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie odpowiadają oni za szkodę spowodowaną przetwarzaniem, ponoszą odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. Administrator lub podmiot przetwarzający, który zgodnie zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądać od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność.

Czynności powierzenia	Odrębne administrowanie
– usługi księgowe, centra rozliczeniowe, – outsourcing w ramach przetwarzania danych w chmurze, – outsourcing administracji pocztą elektroniczną oraz podobnych usług dotyczących danych na stronie internetowej, – outsourcing przechowywania zapasowych kopii bezpieczeństwa lub innego archiwizowania, – niszczenie nośników danych przez usługodawcę, – podmioty zewnętrzne, usługodawcy itd., którym zleca się odczytywanie oraz/lub zbieranie, względnie przetwarzanie opłat za media w mieszkaniach czynszowych (ogrzewanie, prąd, woda itd.).	– doradca podatkowy, adwokat, zewnętrzny lekarz zakładowy, rewident gospodarczy, – agencje windykacyjne przy przeniesieniu roszczeń, – transfer pieniędzy przez instytucje bankowe, usługi płatnicze w przypadku płatności elektronicznych, – działalność administracji budynku, – przesłanie danych uczestnika szkolenia w celu przeprowadzenia szkolenia przez zewnętrznego trenera do organizatora szkolenia lub hotelu, – agencja rekrutacyjna na zlecenie osoby szukającej pracy lub pracodawcy.

2. Powierzenie, udostępnienie czy współadministrowanie?

Wciąż sporym problemem dla wielu firm i instytucji jest określenie, czy udostępnienie danych osobowych, np. swoich pracowników czy klientów, wymaga zawarcia z odbiorcą stosownej umowy powierzenia. Trudne do odróżnienia i często mylone np. z powierzeniem przetwarzania danych osobowych są również relacje współadministrowania. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych osobowych, wówczas stają się oni współadministratorami. W takim przypadku muszą podzielić się odpowiedzialnością oraz obowiązkami w zakresie ochrony tych danych.

Branże, w których działają podmioty przetwarzające

Podmiotem przetwarzającym jest podmiot, który jest odrębnym od administratora bytem prawnym oraz wykonuje operacje przetwarzania danych w imieniu administratora danych (na jego zlecenie). Dlatego więc podmiotami przetwarzającymi nie będą inne podmioty działające pod kierownictwem administratora danych, np. zatrudnione w jego strukturach. Podmiotem przetwarzającym może być zarówno podmiot prywatny (osoba fizyczna prowadząca działalność gospodarczą, osoba prawna), jak i podmiot publiczny.

O konieczności udziału podmiotu zewnętrznego decyduje sam administrator danych, choć w niektórych okolicznościach obowiązek powierzenia danych może wynikać z obowiązujących przepisów, np. w sferze publicznej. Aby stwierdzić, czy dany podmiot będzie miał przymiot podmiotu przetwarzającego, należy odpowiedzieć sobie na pytanie, czy działa w imieniu administratora danych, w jego interesie i w ustalonym przez niego celu. Oczywiście podmiot przetwarzający działający w ramach ustanowionych przez administratora danych ma pewien wpływ na określenie sposobu przetwarzania danych. Wynika to bowiem z faktu, że jest profesjonalistą świadczącym usługi w określonym zakresie. Nadal jednak takie przetwarzanie odbywa się w celach ustalonych przez administratora i w jego imieniu. Decyzję o powierzeniu określonych zadań podmiotowi zewnętrznemu administrator danych może podjąć z różnych przyczyn. Przykładowo, gdy uzna, że takie zlecenie spowoduje, iż pewne czynności podmiot zewnętrzny wykona szybciej, taniej czy skuteczniej. Administratorowi danych może bowiem brakować np. środków technicznych do wykonywania takich czynności samodzielnie (np. w przypadku obsługi informatycznej lub konieczności archiwizowania dużej ilości dokumentów zawierających dane osobowe). W takich przypadkach bardziej opłacalne jest zawarcie umowy z firmą zewnętrzną.

Udostępnienie danych przez administratora

Od powierzenia danych należy odróżnić pojęcie udostępnienia danych. W przypadku udostępnienia dane osobowe przekazywane są innemu podmiotowi, który w stosunku do nich staje się odrębnym administratorem. W tym przypadku ten drugi, odrębny administrator nie działa na zlecenie i w zakresie określonym przez pierwotnego administratora, bowiem sam te cele wyznacza.

Kwestia uznawania banków oraz ośrodków medycyny pracy za podmioty przetwarzające dane osobowe w imieniu administratora danych budzi największe wątpliwości. Banki stoją na stanowisku, iż są samodzielnymi administratorami danych osobowych, również w zakresie danych osobowych pracowników, przekazywanych przez pracodawcę w celu wykonywania czynności bankowych. Bank przy wykonywaniu czynności działa w oparciu o obowiązujące go przepisy prawa, m.in. Prawo bankowe czy ustawy o usługach płatniczych oraz o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. Podobnie rzecz ma się z ośrodkami medycyny pracy. Działają one na podstawie obowiązujących je przepisów, np. na podstawie rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy (Dz. U. z 2016 r. poz. 2067).

Wspólne administrowanie czy powierzenie?

Współadministrowanie bezwzględnie należy odróżnić od powierzenia przetwarzania. W praktyce okazuje się to dość trudne. W obu przypadkach dochodzi bowiem do przetwarzania danych przez więcej niż jeden podmiot. Rozróżnienie, czy w danym przypadku mamy do czynienia z powierzeniem przetwarzania czy też ze współadministrowaniem, musi następować po każdorazowej analizie danej zależności między administratorami i ich wpływie na ustalanie celów i sposobów przetwarzania danych osobowych. Z powierzeniem mamy do czynienia, gdy osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, przetwarza dane osobowe w imieniu administratora. Nie decyduje wraz z nim o celach i sposobach przetwarzania danych, a jedynie przetwarza je w celach określonych wcześniej przez administratora.

W jaki więc sposób ustalić, czy współpraca między podmiotami prowadzi do współadministrowania danymi? Przede wszystkim należy odpowiedzieć sobie na pytanie, czy w praktyce więcej niż jeden podmiot decyduje o celach i sposobach przetwarzania. Współadministrowanie wystąpi, jeżeli przynajmniej dwa podmioty przetwarzają te same dane osobowe (współdzielą zasoby). Takim przykładem będzie prowadzenie wspólnej akcji marketingowej przez dwie firmy, działania ubezpieczycieli i banków, prowadzenie tzw. wielostronnych programów lojalnościowych czy też jednej bazy rekrutacyjnej w grupie przedsiębiorstw. Przy czym, aby takie podmioty mogły zostać uznane za współadministratorów, muszą uzgodnić między sobą kwestie dotyczące przetwarzania danych, związanych z tym obowiązków i zakresu odpowiedzialności. Jeżeli jednak podmioty korzystają z tych samych zasobów, np. z tej samej bazy klientów i przetwarzają ich dane osobowe, ale realizują inne cele i samodzielnie decydują o przetwarzaniu tych danych, wówczas nie stają się współadministratorami, a każdy z nich posiada status odrębnego administratora.

Medycyna pracy

Zgodnie z najnowszymi wytycznymi Prezesa UODO ośrodki medycyny pracy nie są podmiotami przetwarzającymi dane na zlecenie pracodawców, a odrębnymi administratorami przekazanych przez pracodawców danych pracowników kierowanych na badania.

3. Rejestrowanie czynności przetwarzania

Obowiązek rejestrowania czynności przetwarzania przez administratorów danych i podmioty przetwarzające wynika z art. 30 RODO. Prowadzenie rejestru czynności przetwarzania jest jednym z elementów umożliwiających realizację przez administratora zasady rozliczalności. Każdy administrator i podmiot przetwarzający ma obowiązek współpracy z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania operacji przetwarzania.

Kto musi prowadzić rejestry przetwarzania?

Obowiązek prowadzenia rejestru czynności przetwarzania spoczywa na administratorze danych, czyli osobie fizycznej lub prawnej, organie publicznym, jednostce lub innym podmiocie, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Natomiast na podmioty przetwarzające dane osobowe, np. biura rachunkowe, RODO nakłada obowiązek prowadzenia rejestrów wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Są to dwa odrębne rejestry o różnym zakresie informacji. Może zdarzyć się, że jeden podmiot musi prowadzić oba rejestry, tj. rejestr czynności przetwarzania we własnym imieniu jako administrator danych oraz drugi, tj. rejestr wszystkich kategorii czynności przetwarzania, których dokonuje w imieniu administratora danych.

Zasadniczo z obowiązku prowadzenia obu tych rejestrów RODO zwalnia przedsiębiorców lub pomioty zatrudniające mniej niż 250 osób. Zwolnienie to miało na celu ulżyć w powyższych obowiązkach mikro-, małym i średnim przedsiębiorcom. Motyw 13 RODO stanowi bowiem, że: „Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw niniejsze rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników".

Jednocześnie RODO w art. 30 ust. 5 określa, że zwolnienie to nie przysługuje przedsiębiorcom i podmiotom, które zatrudniają mniej niż 250 pracowników, jeżeli czynności przetwarzania, które wykonują:

- mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie mają charakteru sporadycznego,
- obejmują szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych.

Pomimo tego, iż RODO przewiduje zwolnienie dla podmiotów i przedsiębiorców z sektora MŚP, to występowanie przesłanki niesporadycznego przetwarzania danych osobowych powoduje konieczność prowadzenia takich rejestrów. Stanowisko takie znajduje obecnie poparcie w opinii wydanej przez Grupę Roboczą art. 29, która uznała, że brzmienie art. 30 ust. 5 RODO jasno przewiduje, że trzy rodzaje przetwarzania, do których wyjątek nie ma zastosowania, mają charakter alternatywny (lub) i wystąpienie któregokolwiek z nich samodzielnie wywołuje obowiązek prowadzenia rejestru czynności przetwarzania. Jeśli chodzi o przesłankę sporadyczności, to Grupa art. 29 jako przykład podaje małą organizację, która systematycznie przetwarza dane dotyczące swoich pracowników. W rezultacie takie przetwarzanie nie może być uznane za sporadyczne i musi w związku z tym być zawarte w rejestrze czynności przetwarzania. Jednak inne czynności przetwarzania, które w rzeczywistości mają charakter sporadyczny, nie muszą być zawarte w rejestrze czynności przetwarzania, pod warunkiem że jest mało prawdopodobne, by powodowały ryzyko naruszenia praw lub wolności osób fizycznych, i nie obejmują szczególnych kategorii danych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

Rejestry podmiotów przetwarzających

Kolejny problem dotyczy sytuacji, w której administrator danych (np. klient biura rachunkowego) jest zobowiązany do prowadzenia rejestru czynności przetwarzania, natomiast biuro rachunkowe jako przetwarzający, będący np. mikroprzedsiębiorcą, korzysta ze zwolnienia i nie musi prowadzić takich rejestrów. Wydaje się, że ze względu na przesłankę niesporadycznego przetwarzania danych osobowych, należałoby przyjąć konieczność prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. Trudno bowiem uznać, iż biuro rachunkowe przetwarza dane osobowe przekazane przez swoich klientów tylko sporadycznie, zwłaszcza jeżeli jego klientami są duże firmy, zatrudniające powyżej 250 pracowników. Rejestr prowadzony przez podmiot przetwarzający powinien zawierać:

- imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych,
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
- gdy ma to zastosowanie – informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

W odniesieniu do każdego z administratorów wskazane jest zatem nazwanie poszczególnych powierzeń (zleceń), a zatem rodzaju usług, jakie podmiot przetwarzający na podstawie zawartych umów wykonuje na rzecz poszczególnych administratorów. Uporządkowanie czynności wykonywanych w ramach powierzenia w kategorie, czyli ich pogrupowanie pod względem rodzaju usług świadczonych przez podmiot przetwarzający, umożliwi łatwy przegląd powierzeń, zwłaszcza w przypadku podmiotów, które działają na rzecz wielu administratorów danych lub świadczą wiele różnych usług w zakresie przetwarzania danych. Taką kategorią czynności przetwarzania będzie już samo przechowywanie dokumentacji podatkowej, księgowej, kadrowej i medycznej, a także prowadzenie wspomnianej dokumentacji.

Rejestr czynności przetwarzania danych osobowych prowadzony przez administratora danych powinien zawierać:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- gdy ma to zastosowanie, przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

4. Bez umowy powierzenia z zakładem medycyny pracy

Firma planuje zawrzeć umowę z zakładem medycyny pracy na badania pracowników. Czy z takim podmiotem należy również zawrzeć umowę powierzenia w zakresie ochrony danych osobowych?

NIE. Zgodnie z najnowszymi interpretacjami, również UODO, zakłady medycyny pracy nie są podmiotami przetwarzającymi w rozumieniu art. 4 pkt 8 ogólnego rozporządzenia o ochronie danych osobowych. Takim podmiotem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

O konieczności scedowania niektórych obowiązków na rzecz innego pomiotu decyduje sam administrator danych (w niektórych okolicznościach taki obowiązek może wynikać z obowiązujących przepisów, np. w sferze publicznej). Co istotne, pomimo przekazania tych obowiązków o celach przetwarzania danych osobowych nadal decyduje administrator danych, on również odpowiada za prawidłową ochronę danych osobowych, w stosunku do których jest administratorem. Podmiot przetwarzający może natomiast dokonywać tylko takich czynności przetwarzania na danych osobowych, które mu powierzono, do jakich obliguje go umowa.

Ośrodki medycyny pracy nie są podmiotami przetwarzającymi. W zakresie wykonywanych czynności są odrębnymi administratorami danych. Zakład medycyny pracy nie przetwarza danych w imieniu pracodawcy, tylko realizuje własne cele wynikające z obowiązków prawnych. Pomimo skierowania pracownika przez pracodawcę, to zakład medycyny pracy samodzielnie zbiera dane medyczne pacjenta i realizuje szereg celów wynikających z obowiązujących go przepisów, np. rozporządzenia Ministra Zdrowia i Opieki Społecznej w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy, a także rozporządzenia Ministra Zdrowia w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów. W związku z powyższym nie ma potrzeby zawierania umowy powierzenia przez pracodawcę z takim zakładem.

5. Biegły rewident jest administratorem danych

Jestem biegłym rewidentem. Prowadząc audyt lub badając sprawozdanie finansowe, mam do czynienia z różnego rodzaju danymi osobowymi. Czy w takich przypadkach jestem administratorem takich danych, czy też przysługuje mi status podmiotu przetwarzającego?

Uchwycenie różnicy między tym, czy przetwarzając dane osobowe, dany podmiot jest w stosunku do nich samodzielnym administratorem, czy też podmiotem przetwarzającym w imieniu administratora, sprawia wciąż sporo kłopotów. Zgodnie z definicjami zawartymi w RODO, administratorem danych jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Natomiast podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Przeprowadzając swoje czynności, audytorzy (firmy audytorskie) oraz biegli rewidenci działają na podstawie obowiązujących ich przepisów prawa. Chodzi tu przede wszystkim o ustawę o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2019 r. poz. 1421 ze zm.) oraz o rozporządzenie Parlamentu Europejskiego i Rady (UE) 537/2014 w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych (...). Natomiast w zakresie ochrony przetwarzanych danych osobowych muszą stosować się do przepisów RODO.

Aby stwierdzić status podmiotu, który przetwarza dane osobowe, należy odpowiedzieć sobie na pytanie, czy przetwarzając dane osobowe, podmiot realizuje własne cele (i sam je sobie określa), czy też przetwarza dane na zlecenie administratora, realizując cel innego administratora danych. Jak czytamy na stronie Urzędu Ochrony Danych Osobowych www.uodo.gov.pl, w sekcji Zadania IOD: „Ustawa (...) o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym wskazuje, że istotą tego zawodu jest niezależność i obiektywizm w przeprowadzaniu badania. Biegły rewident jest obowiązany w szczególności: postępować zgodnie ze złożonym ślubowaniem; przestrzegać krajowych standardów wykonywania zawodu, wymogów niezależności oraz zasad etyki zawodowej. Dodatkowo art. 2b tej ustawy wskazuje wprost na sposoby zabezpieczenia danych przetwarzanych w ramach działalności firm audytorskich oraz biegłych rewidentów. Tym samym, charakter relacji pomiędzy firmami audytorskimi oraz biegłymi rewidentami a ich klientami wskazuje na to, że występują one w roli samodzielnych administratorów".

W związku z tym należy uznać, iż przetwarzając dane osobowe w celu przeprowadzenia audytu czy też czynności właściwych dla biegłych rewidentów, Czytelnik ma status samodzielnego administratora i to on w odniesieniu do tych danych odpowiada za ich bezpieczeństwo.

6. Zgoda pracowników na przetwarzanie ich danych przez biuro rachunkowe

Biuro rachunkowe świadczy usługi w zakresie prowadzenia akt osobowych i naliczania wynagrodzeń. Ma podpisane umowy powierzenia. Czy jako podmiot przetwarzający ma obowiązek uzyskać zgodę od pracowników swoich klientów na przetwarzanie ich danych osobowych?

Biuro, wykonując wspomniane w pytaniu czynności, posiada przymiot podmiotu przetwarzającego. Przetwarza bowiem dane osobowe na zlecenie innych podmiotów będących administratorami tych danych. Podstawą przetwarzania danych w takich przypadkach musi być umowa powierzenia zawarta pomiędzy administratorem danych a podmiotem przetwarzającym.

Umowa ta upoważnia pracowników biura rachunkowego do przetwarzania danych osobowych pracowników podmiotu będącego klientem biura rachunkowego. Oczywiście to przetwarzanie może odbywać się tylko w zakresie określonym przez administratora tych danych. Jednym z obowiązków, jakie RODO nakłada na podmioty przetwarzające, jest zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. To zaś oznacza, że osoby dokonujące przetwarzania danych osobowych w biurze rachunkowym Czytelników muszą posiadać stosowne upoważnienia do przetwarzania danych osobowych.

Natomiast pracownicy klientów biur rachunkowych nie muszą udzielać dodatkowych zgód na przetwarzanie ich danych osobowych przez takie podmioty.

W umowie powierzenia podmiot przetwarzający zobowiązuje się m.in. do:

- podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomagania administratorowi wywiązać się z tych obowiązków,
- przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego,
- pomagania administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w RODO,
- usunięcia danych lub do zwrotu danych administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora,
- udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów.

7. Relacja pracodawcy z bankiem

Dane osobowe naszych pracowników przekazywane są do banków, celem dokonania przelewów wynagrodzeń. Dane te obejmują: imię, nazwisko, numer konta bankowego, nazwę naszej firmy. Czy bank powinien zawrzeć z nami umowę powierzenia?

Obecnie obowiązujące przepisy ogólnego rozporządzenia o ochronie danych nie dają jednoznacznej odpowiedzi na to pytanie. Należy stwierdzić, że podmiotem przetwarzającym, z którym należy zawrzeć umowę powierzenia, jest podmiot, który przetwarza dane osobowe w imieniu administratora danych. Natomiast administratorem danych osobowych jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Dla zrozumienia instytucji powierzenia przetwarzania danych osobowych najlepszym przykładem są biura rachunkowe i osoby świadczące firmom usługi informatyczne. Podmioty te wykonują zadania zlecone przez administratora danych (osobę prowadzącą działalność gospodarczą, spółkę) i pracują na danych przekazanych im przez administratora. Dlatego tak ważny jest wybór odpowiedniego podmiotu przetwarzającego, który zapewnia właściwą ochronę przekazywanych danych osobowych. Podmiot przetwarzający nie decyduje o celach i zakresie przetwarzanych danych osobowych, cele te wyznacza administrator danych. Podmiot przetwarzający działa w zakresie wynikającym z zawartej z administratorem danych umowy powierzenia. W sytuacji gdy pracodawca zawiera z bankiem umowę, w ramach której bank świadczy usługi (dokonuje przelewów wynagrodzeń) niektórzy uznają, że bank może być uznany za podmiot przetwarzający. Działa bowiem tylko w celu i w zakresie określonym przez pracodawcę i nie decyduje sam o tych celach.

Banki mają jednak w tym zakresie inne zdanie. Uznają się za samodzielnych administratorów danych. Jako podstawę prawną przetwarzania danych osobowych pracowników wskazują art. 6 ust. 1 lit. f) RODO, czyli przetwarzanie danych jako niezbędne do celów wynikających z prawnie uzasadnionych interesów administratora (banku). Tym interesem jest realizacja umowy zawartej z pracodawcą. W takim przypadku administratorem danych pracowników jest zarówno pracodawca, jak i bank w zakresie wynikającym z zawartej z pracodawcą umowy. Zdarza się jednak, że bank, stawiając siebie w roli administratora danych, jako podmiot przetwarzający (procesora) ustanawia pracodawcę i zobowiązuje go do podpisania umowy powierzenia.

Prezes Urzędu Ochrony Danych Osobowych również stoi na stanowisku, iż w przypadku umów zawieranych przez pracodawców z bankami, nie mamy do czynienia z umową powierzenia. Bank staje się odrębnym administratorem przekazanych mu danych. Na stronie urzędu www.uodo.gov.pl czytamy: „Pracodawca zawiera z bankiem umowę o świadczenie usług bankowych i to na jej podstawie udostępnia dane swoich pracowników w celu dokonania przelewów wynagrodzeń. Bank realizuje zadania wynikające z przepisów Prawa bankowego i w momencie otrzymania od pracodawcy danych pracowników w celu świadczenia usług bankowych, staje się administratorem tych danych".

8. Zawieranie umów o benefity dla pracowników

Instytucja chce zaoferować swoim pracownikom karnety na siłownię, basen i lodowisko. Czy firma, z którą zawrzemy umowę o dostarczanie tych benefitów, będzie podmiotem przetwarzającym? Na jakiej zasadzie mamy jej przekazywać dane osobowe naszych pracowników?

Przede wszystkim należy stwierdzić, iż korzystanie przez pracowników ze wspomnianych benefitów jest w pełni dobrowolne, co oznacza, że pracodawca nie może udostępnić danych osobowych pracowników bez ich wiedzy i zgody na rzecz podmiotów świadczących te usługi. Udostępnienie danych osobowych przez pracodawcę powinno odbywać się na podstawie zgody wyrażonej przez pracownika, zgodnie z art. 6 ust. 1 lit. a) RODO.

Podmioty te stają się administratorami danych osobowych osób w zakresie oferowanych przez siebie usług. Nie są podmiotami przetwarzającymi, gdyż nie przetwarzają danych osobowych pracowników w imieniu pracodawcy. Oferują bowiem zupełnie inne usługi, niezależne od działań pracodawcy. Stąd mamy do czynienia z relacją ADO-ADO (tj. dwóch niezależnych administratorów).

Istota powierzenia przetwarzania danych osobowych

Konsekwencją uznania podmiotu za administratora danych osobowych jest konieczność stwierdzenia, że takie podmioty są zobowiązane do informowania osób, których dane dotyczą o okolicznościach wskazanych w art. 13 RODO, np. w deklaracji przystąpienia. Jednocześnie nie ma tu zastosowania instytucja powierzenia przetwarzania danych osobowych. Podkreślić należy, że istota powierzenia przetwarzania danych osobowych polega m.in. na tym, że nie jest wymagane uzyskanie zgody osoby, której dane dotyczą, na powierzenie jej danych.

źródło: www.uodo.gov.pl

9. Wysokość kar w umowie powierzenia przetwarzania danych osobowych

Świadczymy usługi w zakresie niszczenia dokumentacji i nośników danych. Spółka z o.o., którą obsługujemy, przedstawiła nam swoją wersję umowy powierzenia przetwarzania danych osobowych. W umowie zawarto szereg kar finansowych mających zastosowanie w przypadku naruszenia któregokolwiek z postanowień dotyczących ochrony danych osobowych ujętych w umowie albo w przypadku naruszenia przepisów obowiązującego prawa, w tym RODO. Czy takie zapisy są ważne?

Administratorzy danych mogą korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Tak stanowi art. 28 ust. 1 RODO.

Przetwarzanie przez podmiot przetwarzający może odbywać się tylko na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora. Taka umowa powinna określać przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora. W umowie tej podmiot przetwarzający zobowiązuje się m.in. do pomagania administratorowi w wywiązywaniu się z obowiązków, jakie nakłada na niego RODO. Ponadto udostępnia mu wszelkie informacje niezbędne do wykazania spełnienia ciążących na podmiocie przetwarzającym obowiązków. Co więcej, zobowiązuje się umożliwiać administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji.

W związku z tym, że administratorzy danych mają obowiązek zawierania umów tylko z podmiotami przetwarzającymi, które gwarantują przestrzeganie zasad właściwej ochrony danych osobowych, w umowach powierzenia zabezpieczają oni prawidłowość nałożonych na podmioty przetwarzające obowiązków karami umownymi. Oczywiście zastrzeganie kar umownych zależy od woli obu stron.

Możliwość zawierania w umowach kar umownych w przypadku zobowiązań niepieniężnych (a z takimi mamy tu do czynienia) dopuszcza art. 483 § 1 Kodeksu cywilnego (Dz. U. z 2019 r. poz. 1145 ze zm.). Stanowi on, że można zastrzec w umowie, że naprawienie szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania niepieniężnego nastąpi przez zapłatę określonej sumy (kara umowna).

Obowiązujące przepisy Kodeksu cywilnego nie określają maksymalnych wysokości kar umownych. Dlatego często zdarza się, że są one bardzo wysokie. Kary powinny być ustalone na takim poziomie, by zabezpieczały ewentualne roszczenia kontrahenta, a jednocześnie, by ich wysokość była możliwa do przyjęcia przez drugą stronę.

W przypadku kary umownej, nieadekwatnej do wysokości poniesionej szkody, zobowiązany może wnosić o obniżenie jej wysokości przez sąd w drodze tzw. miarkowania.

10. Administrator danych może skontrolować podmiot przetwarzający

Świadczymy usługi archiwizacji. Działamy na podstawie umów powierzenia zawieranych z klientami. Jeden z klientów zapowiedział przeprowadzenie w naszym biurze kontroli zasad przestrzegania bezpieczeństwa ochrony danych. Czy ma do tego prawo? Jeżeli tak, to czy będzie mógł mieć wgląd do naszej wewnętrznej dokumentacji?

Zgodnie z zasadą rozliczalności wyrażoną w art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie przepisów prawa i musi być w stanie wykazać ich przestrzeganie. Zasada ta ma zastosowanie zarówno do przetwarzania realizowanego samodzielnie przez administratora, jak i przetwarzania w jego imieniu przez podmiot przetwarzający.

Każdy administrator danych, który korzysta z usług podmiotów przetwarzających, ma obowiązek wybierać tylko takie podmioty, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Tak stanowi art. 28 ust. 1 RODO. Przetwarzanie przez podmiot przetwarzający musi odbywać się na podstawie umowy lub innego instrumentu prawnego, które określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Umowa musi określać m.in., iż podmiot przetwarzający jest zobowiązany udostępniać administratorowi wszelkie informacje niezbędne do wykazania spełnienia jego obowiązków oraz umożliwiać administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczyniać się do nich.

W związku z powyższym, administrator, jeszcze przed zawarciem umowy o przetwarzanie danych, powinien mieć możliwość sprawdzenia, czy podmiot, z którym chce współpracować, realizuje obowiązki związane z zapewnieniem rzetelnej ochrony przekazywanych mu danych. Prawo dostępu do takich informacji oraz przeprowadzania audytów przysługuje administratorowi również w trakcie realizacji umowy powierzenia. W tym celu w art. 28 ust. 3 lit. h) RODO na podmiot przetwarzający zostały nałożone obowiązki udostępniania administratorowi wszelkich informacji potwierdzających spełnienie wymogów RODO, a także umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji.

Administrator jest bowiem zobowiązany do stałej kontroli, czy podmiot przetwarzający przetwarza dane zgodnie z prawem. Kontrole te mogą być przeprowadzane również doraźnie, np. w przypadku wystąpienia naruszenia ochrony powierzonych danych osobowych. Inne postanowienia umowy powierzenia, które ograniczają te prawa administratora uznaje się za niezgodne z RODO. Również utrudnianie lub ograniczanie administratorowi możliwości przeprowadzania kontroli u podmiotu przetwarzającego lub ograniczanie jej zakresu jest niedopuszczalne.

11. Postępowanie podmiotu przetwarzającego w przypadku naruszenia ochrony danych

Jesteśmy dostarczycielami usług hostingowych. Mamy zawarte umowy powierzenia z kilkoma różnymi firmami. Jeden z pracowników wysłał przez pomyłkę dokumenty dotyczące jednego z klientów do wszystkich pozostałych podmiotów, których dane przetwarzamy w trakcie realizacji naszych usług. Jak powinniśmy postąpić w sytuacji wystąpienia u nas naruszenia ochrony danych osobowych?

Administrator danych ponosi odpowiedzialność za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. Oznacza to, że mimo zawarcia umowy powierzenia, na administratorze danych nadal ciążą obowiązki związane z ochroną przekazywanych danych osobowych. Dlatego tak ważne jest wybieranie tylko tych podmiotów przetwarzających, które gwarantują taką ochronę przetwarzanym danym. W szczególności posiadają wiedzę fachową, wiarygodność i zasoby niezbędne do wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania (motyw 81 RODO). Ponadto administrator ma obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z RODO oraz, że są skuteczne. Natomiast zgodnie z art. 28 ust. 3 lit. f) RODO, umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z tych obowiązków.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki zgłasza je administratorowi. Co oznacza najszybciej, jak to możliwe. Przy czym warto w zawieranych umowach powierzenia dokonać zapisu takiego terminu wywiązywania się z obowiązku informowania administratora o wystąpieniu incydentu naruszenia ochrony danych. Prezes UODO na stronie www.uodo.gov.pl zwraca uwagę, że jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, a dany incydent wywiera wpływ na wszystkich z nich, podmiot przetwarzający jest zobowiązany do zgłoszenia naruszenia bez zbędnej zwłoki każdemu z tych administratorów. Pamiętać należy, że brak odpowiedniego działania po stronie podmiotu przetwarzającego w sytuacji naruszenia ochrony danych osobowych może skutkować zastosowaniem przez Prezesa UODO wobec podmiotu przetwarzającego uprawnień określonych w art. 58 RODO. Urząd Ochrony Danych Osobowych zwraca uwagę, iż nie wszystkie podmioty, przy pomocy których administratorzy przetwarzają dane osobowe, gwarantują odpowiednie bezpieczeństwo danych osobowych oraz szybkie i skuteczne rozwiązania służące prawidłowemu wywiązywaniu się z obowiązków określonych w art. 33 i 34 RODO.

Przykład

U podmiotu przetwarzającego doszło do naruszenia ochrony danych osobowych, co wymaga podjęcia działań mających na celu jak najszybsze zablokowanie nieuprawnionego dostępu do tych danych. Naruszenie to dotyczy danych przetwarzanych w ramach powierzenia.

W związku z zaistniałym zdarzeniem administrator powinien wydać odpowiednie polecenie podmiotowi przetwarzającemu i zadbać o to, aby żądania organu nadzorczego wydane w stosunku do niego zostały jak najszybciej i skutecznie zrealizowane.

12. Umowa powierzenia dla zewnętrznej firmy szkolącej

Jako pracodawca zastanawiam się nad zatrudnieniem zewnętrznej firmy do prowadzenia szkoleń z zakresu bhp. Czy z taką firmą należy zawrzeć umowę powierzenia, czy wystarczy upoważnić osobę prowadzącą takie szkolenie do przetwarzania danych osobowych pracowników?

Podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Cele i zakres tego przetwarzania określa administrator danych. W celu określenia, czy dany podmiot będzie podmiotem przetwarzającym, należy odpowiedzieć na pytanie, czy administrator danych mógłby powierzane czynności przeprowadzić we własnym zakresie. Odpowiedź będzie twierdząca, bowiem wielu pracodawców do zadań służby bhp deleguje wyspecjalizowanego pracownika. W takim przypadku osoba będąca jednocześnie pracownikiem przetwarza dane osobowe innych pracowników zatrudnionych w zakładzie pracy wyłącznie z upoważnienia administratora.

Jeżeli jednak administrator danych zdecyduje się wybrać zewnętrzną firmę, wówczas konieczne wydaje się zawarcie umowy powierzenia danych osobowych. Taka umowa może być częścią umowy na usługi lub zlecenia. Nie musi być koniecznie odrębną umową, ale musi zawierać wszystkie elementy określone w przepisach RODO.

Takie stanowisko potwierdza również Ministerstwo Cyfryzacji w publikacji „RODO w administracji", w której czytamy, że: „Jeżeli administrator zdecydował się jednak na zewnętrzny podmiot, który obsługuje go w tym zakresie (bhp – przyp. red.), należy podpisać umowę powierzenia. W takim przypadku administrator powierza bowiem innemu podmiotowi zadanie, które mógłby zrealizować samodzielnie".

Podmiot ten musi upoważnić swoich pracowników do przetwarzania danych osobowych otrzymanych do przetwarzania (dane otrzymane od swojego klienta).

Jednocześnie jednak w publikacji tej zwraca się uwagę, iż dopuszczalne było niezawieranie umowy powierzenia w sytuacji, gdy pracownik zewnętrznej firmy szkolącej z zakresu bhp przetwarzałby dane pracowników firmy w jej siedzibie, a firma szkoląca nie miałaby do czynienia z tymi danymi poza firmą. Wystarczające byłoby wtedy upoważnienie tego szkolącego pracownika do przetwarzania danych.

Podstawa prawna

Rozporządzenie Parlamentu Europejskiego (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)